添付資料

【今月の呼びかけ】

「 深刻化する偽セキュリティ対策ソフトの被害！ 」

この数か月にわたり、過去の「呼びかけ」で何回か取り上げている「偽セキュリティ対策ソフト」型ウイルスによる被害の相談が増加しています（図 1-1 を参照）。最近の「偽セキュリティ対策ソフト」型ウイルスに関する相談の傾向として、復旧のための操作ができなくなるなど、被害に遭ったパソコンの症状が以前より深刻化しています。また、感染経路が「ガンブラー」(※1)の手口によるものだと考えられる事例が多く、セキュリティ対策が不十分なパソコンでは、改ざんされたウェブサイトを閲覧しただけで、この種のウイルスに感染させられてしまう可能性があります。

「偽セキュリティ対策ソフト」型ウイルスの被害に遭わないための対策は、このウイルスに限った特別なものではなく、基本的なセキュリティ対策を漏れなく実施することです。ここでは、被害の実例を紹介し、対策について説明します。

(※1) ガンブラー： 「"ガンブラー" の手口を知り、対策を行いましょう」（IPA, 2010 年 2 月の呼びかけ）を参照
http://www.ipa.go.jp/security/txt/2010/02outline.html#5

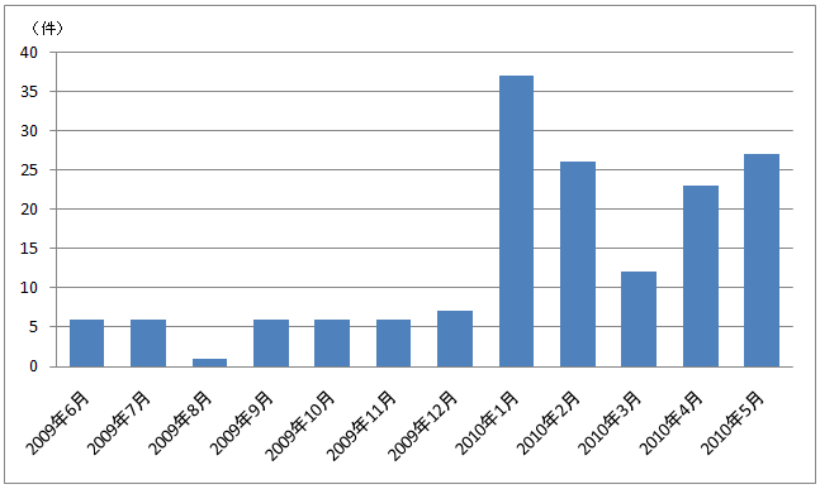

図 1-1：「偽セキュリティ対策ソフト」型ウイルスに関する過去 1 年分の相談件数

（1）「偽セキュリティ対策ソフト」型ウイルスの概要

「偽セキュリティ対策ソフト」型ウイルスとは、“ウイルスに感染している”といった虚偽の警告メッセージを表示し、それらを解決するには有償版の製品が必要であるとして、例えばクレジットカード番号の入力を要求し、金銭を騙し取るタイプのウイルスです。正規のセキュリティ対策ソフトと見分けがつかないような見栄えの画面と共に、「Security essentials 2010」や「XP Smart Security 2010」など、いかにも本物らしいソフトの名称（他にも多くのソフト名が確認されています）が表示されるため、注意が必要です。

この種のウイルスの中には、ウイルスの駆除やパソコンからのデータの退避（バックアップ）作業を妨害するものもあるため、深刻な被害となる場合があります。「偽セキュリティ対策ソフト」型ウイルスについての詳細は、2009 年 11 月の呼びかけも参照してください。

（ご参考）
「 偽のセキュリティ対策ソフトの脅威が再び拡大！ 」（IPA, 2009 年 11 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2009/11outline.html#5

（2）被害の実例

具体的な相談と届出の事例を示します。次の図 1-2 は、下記の事例で相談者が感染させられた「偽セキュリティ対策ソフト」型ウイルスの画面（一部）です。

【事例1】偽セキュリティ対策ソフト
「Security essentials 2010」の画面

【事例2】偽セキュリティ対策ソフト
「Control center」の画面

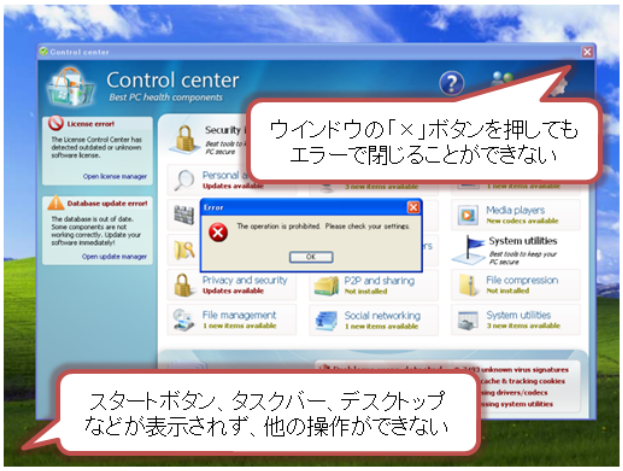

図 1-2：「偽セキュリティ対策ソフト」型ウイルスの感染画面例

【事例 1】

相談内容	**ウェブサイトを閲覧していたら、突然英語の画面になり**、再起動させても消えない。「YOUR SYSTEM IS INFECTED」などと表示されている。「セーフモード」(※2)で起動しても、英語の警告メッセージが表示される。「タスクマネージャ」(※3)や「システムの復元」(※4)も起動できず、パソコンが正常に利用できない。
ソフト名	Security essentials 2010
解説	相談者が感染させられた「Security essentials 2010」は、5 月に最も相談が多かったウイルスです。マイクロソフト社が提供しているセキュリティ対策ソフトの「Microsoft Security Essentials」とは関係なく、紛らわしい名前で有用なソフトと勘違いさせようとしていると考えられます。このウイルスについては、今年の 2 月から IPA へ相談が寄せられています。

(※2) セーフモード： パソコンの復旧作業などを行うための Windows の特殊な起動方法。

(※3) タスクマネージャ： パソコン上で動作しているプログラムの一覧表示や、任意のプログラムの停止を行うためのツール。

(※4) システムの復元： Windows に付属している、パソコンの設定などを以前の状態に巻き戻すツール。

【事例 2】

相談内容	パソコンを起動すると、ウイルス対策ソフトのライセンスが切れているため料金を支払うよう書かれた画面が表示されるようになった。「セーフモード」でも同じ状況で、それ以上の操作ができない。パソコン内に必要な情報が残っており、初期化するわけにもいかなかったため、クレジットカード番号を入力した。そうすると、操作できるようにはなったが、デスクトップ上のファイルが消えていた。
ソフト名	Control center　（Control center - Best PC health components）
解説	パソコンやその中のデータだけでなく、金銭的な被害まで発生した事例です。ウイルスの作者は、感染させたパソコンを操作不能に陥れることで、料金を支払わせようとしています。本件の感染経路は不明ですが、感染の直前に**不審な添付ファイルの付いたメールを開いた**、とのことでした。なお、ライセンスを購入しても状況が改善する保証はなく、支払いをすべきではありません。

【事例 3】

相談内容	インターネットを利用していたら、画面に英文のメッセージが大量に表示され、正しく動作しなくなった。パソコンのメーカーに問い合わせたところ、初期化を指示されたので、その通りにした。「Security Tool」というものらしいが、対処はこれで良かったのか。
ソフト名	Security Tool
解説	「Security Tool」は水色の画面が特徴的なウイルスで、IPA へは 2009 年の末ごろから相談が寄せられています。対処としては、初期化で問題ありません。ただ、**セキュリティ対策が不十分な状態でウェブサイトを閲覧していて感染した**とのことで、相談者の方が自分自身でセキュリティ対策を実施できるようにならなければ、また同じ被害に遭う可能性があります。

このほか、5 月に相談・届出があった「偽セキュリティ対策ソフト」型ウイルスは次の通りです。多種のウイルスが広くばら撒かれていることが推測されます。

- XP AntiMalware 2010
- XP Smart Security 2010
- Live Security Suite
- Data Protection
- Digital Protection
- Desktop Security 2010

事例に似た症状が現れたり、図 1-2 のような身に覚えのないウイルススキャンの画面が表示された場合は、「偽セキュリティ対策ソフト」型ウイルスに感染させられた可能性が高く、加えて、「偽セキュリティ対策ソフト」型ウイルス以外のウイルスも同時にパソコンに侵入している可能性があります。次の（3）に示す対処を実施してください。

このような「偽セキュリティ対策ソフト」型ウイルスなどの被害に遭わないための事前対策については、（4）を参照してください。

（3）感染時の対処

事例で示したように、「偽セキュリティ対策ソフト」型ウイルスに一旦感染させられてしまうと、復旧や駆除が難しい場合があります。感染時の対処の指針を次に示しますので、これを参考に、症状の改善や復旧を試みてください。

- パソコンが操作できる状態であれば、最新のウイルス対策ソフトでパソコンのスキャンを行い、ウイルスの駆除を試みます。
  - ウイルス対策ソフトが手元にない場合は、各ウイルス対策ソフトのベンダーがウェブサイトで提供している「オンラインスキャン」を使うこともできます。
- ウイルス対策ソフトでの駆除ができない場合は、「システムの復元」（下記（iii）を参照）による復旧を試みます。
- パソコンが操作できない、ウイルス対策ソフトによる駆除ができない、あるいは「システムの復元」がうまくいかない、といった場合は、パソコンを「セーフモード」（下記（ii）を参照）で起動した上で、これらの作業を再度試みます。
  - パソコンのシャットダウン操作すらできない状態であれば、本体の電源ボタンをしばらく押し続け、強制的に電源を切ってから、「セーフモード」での起動を行います。
- これらの作業で復旧しない場合は、パソコンの初期化（購入した時の状態に戻す作業）を行います。「偽セキュリティ対策ソフト」型ウイルスに感染している状態のパソコンは、例えある程度操作ができたとしても、ウイルスによる情報漏えい等が発生する可能性があるため、<u>そのまま使用することは危険</u>です。

以下、対処における個別の注意点や手順について（i）～（iv）に示します。

（i）「偽セキュリティ対策ソフト」のライセンス料は支払わないこと

ライセンス料を支払ったとしても、状況が改善するとは限りません（事例 2 を参照）。クレジットカード番号を入力した場合は、その情報が更に悪用される可能性もあります。悪意のある人物の行為を助長することにもなりかねないため、料金を支払うことは避けてください。

（ii）「セーフモード」の利用

Windows を「セーフモード」で起動することで、ウイルスの動作を制限できる場合があり、通常の状態ではウイルスによる妨害で正しく動作しなかったツールを利用できる可能性があります。「セーフモード」を利用し、**データのバックアップ**、**ウイルス対策ソフトによる駆除**、または**「システムの復元」**などを試してください。

「セーフモード」の利用方法については、下記のウェブページを参照してください。パソコンの機種により「セーフモード」での起動方法が異なる場合がありますので、不明な点はパソコンのメーカーへお問い合わせください。

（ご参考）

「Windows XP を セーフ モードで起動する方法」（Windows XP）（マイクロソフト社）
http://support.microsoft.com/kb/880414/ja

「コンピュータをセーフ モードで起動する」（Windows Vista）（マイクロソフト社）
http://windows.microsoft.com/ja-jp/windows-vista/Start-your-computer-in-safe-mode

「コンピューターをセーフ モードで起動する」（Windows 7）（マイクロソフト社）
http://windows.microsoft.com/ja-JP/windows7/Start-your-computer-in-safe-mode

（iii）「システムの復元」による復旧

最新のウイルス対策ソフトを使用しても症状が治まらない場合、「システムの復元」を行うことで、状況を改善できる場合があります。「システムの復元」とは、Windows XP、Windows Vista、Windows 7 に付属しているツールで、パソコンの動作が不安定になるなど、使用に支障がある状態に陥った場合に、以前の状態に戻すことができる機能です。

（ご参考）

「Windows XP 機能別紹介：システムの復元」（Windows XP）（マイクロソフト社）
http://www.microsoft.com/japan/windowsxp/pro/business/feature/performance/restore.mspx

「システムの復元とは」（Windows Vista）（マイクロソフト社）
http://windows.microsoft.com/ja-JP/windows-vista/What-is-System-Restore

「Windows 7 の機能：システムの復元」（Windows 7）（マイクロソフト社）
http://windows.microsoft.com/ja-JP/windows7/products/features/system-restore

なお、下記のウェブページにて、Windowsを「セーフモード」で起動し、「システムの復元」を実施するための具体的な手順を案内しています。

（ご参考）

「Windows での「システムの復元」の実施手順」（IPA）
http://www.ipa.go.jp/security/restore/

（iv）パソコンの初期化

症状が改善しない場合はパソコンの初期化を行ってください。

なお、「偽セキュリティ対策ソフト」型ウイルスでは、複数のウイルスに感染させられている場合があり、復旧できたように見えている場合でも、ウイルスの一部がパソコンに残っている可能性

はゼロではありません。全てのウイルスを確実に消去するために、IPA では原則として初期化を推奨しています。特に、パソコンの動作が不安定であったり、使用していて違和感を覚えた場合は、初期化を検討してください。

初期化を実施する場合、パソコン内のデータは全て消えてしまいますので、通常の操作が可能であれば、できる限り重要なデータのバックアップを取得することを勧めます。初期化の手順については、パソコンの取扱説明書に記載されている「購入時の状態に戻す」などの手順を参照してください。

なお、初期化を行った直後は、パソコンのセキュリティ対策が不十分な状態となります。再び被害に遭うことのないよう、下記（4）の事前対策を確実に実施してください。また、バックアップしたデータを初期化したパソコンに戻す前に、必ずウイルスチェックを行ってください。

（4）事前対策

パソコンのセキュリティ対策に不備が有る場合、インターネット接続中には、今回紹介した事例のような被害に繋がる危険にさらされています。「偽セキュリティ対策ソフト」型ウイルスに限らず、ウイルス全般への防御策として、次に挙げる基本的な対策を漏らさず実施してください。

（i）データの定期的なバックアップ

パソコンの故障など、原因はウイルスに限りませんが、パソコン内のデータはいつでも失われる可能性があることを意識し、重要なデータは定期的にバックアップを行ってください。今回取り上げた「偽セキュリティ対策ソフト」型ウイルスの中には、パソコンからのデータのバックアップ作業を妨害するものもあり、被害に遭った後では手遅れとなってしまう場合があります。

（ii）ウイルス対策ソフトの導入

ウイルス対策ソフトは万能ではありませんが、重要な対策の一つです。ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保つことで、ウイルスの侵入阻止や、侵入してしまったウイルスの駆除ができます。近年のウイルスは、パソコンの画面の見た目では感染していることが分からないものが多いため、ウイルスの発見と駆除には、ウイルス対策ソフトが必須です。

一般利用者向けのウイルス対策ソフトとしては、ウイルスの発見と駆除だけでなく、危険なウェブサイトを閲覧しようとした時にブロックを行う機能などを備える、「統合型」と呼ばれるものを推奨します。

（iii）脆弱性の解消

「ガンブラー」の手口などで使われる、ウェブサイトを閲覧するだけでウイルスに感染させられてしまう「ウェブ感染型ウイルス」は、パソコン内にある**「ウイルスの侵入を許してしまう弱点」**、すなわち**脆弱性**を悪用して侵入してきます。従って、この脆弱性を解消することが、重要な対策の一つです。

脆弱性は、OS（Windowsなど）、ブラウザ（Internet Explorerなど）、その他のアプリケーションソフト、それぞれに存在する可能性があります。パソコンに導入しているソフトウェアについては、できる限り全てを最新版に更新し、脆弱性を解消しましょう。

ソフトウェアの更新の方法について、次に補足します。

- Windows（OS 本体）、Internet Explorer、Microsoft Office（Word や Excel）の更新
  - パソコンの設定によっては「自動更新」の機能がオンになっており、その場合は自動的に最新版に更新されます。手動で更新を行う場合は、「Windows Update」または「Microsoft Update」を使用します。詳しくは、下記のマイクロソフト社のウェブページを参照してください。
  - （ご参考） 「Microsoft Update 利用の手順」（マイクロソフト社）
    http://www.microsoft.com/japan/security/bulletins/j_musteps.mspx

- 「MyJVN バージョンチェッカ」による確認
  - IPA では、Adobe Flash Player など、ウイルスによって狙われることが多いソフトウェアについて、それらがパソコンに導入されているか、および最新版となっているか否かをチェックできるツールを公開しています。詳しくは、下記の「MyJVN バージョンチェッカ」のウェブページを参照してください。また、「MyJVN バージョンチェッカ」の使い方や、個々のソフトウェアを最新版にする手順については、下記の「ホームページからの感染を防ぐために」のページを参照してください。
  - （ご参考） 「MyJVN バージョンチェッカ」（IPA）
    http://jvndb.jvn.jp/apis/myjvn/#VCCHECK
    ※ 2010 年 6 月現在、Windows XPとVistaに対応しています。
  - （ご参考） 「ホームページからの感染を防ぐために」（CCC）
    https://www.ccc.go.jp/detail/web/index.html
- その他のソフトウェア
  - ソフトウェアの更新の方法は、それぞれ異なります。自分のパソコンに導入されているソフトウェアを把握し、定期的に更新を行うことが理想です。パソコン初心者がすぐに実施することは難しいですが、自己防衛のために知識や操作方法の習得を心掛けてください。
- 脆弱性の情報の収集
  - IPA では、一般利用者の多いソフトウェアに脆弱性が発見された場合、注意喚起を行っています。定期的に下記の「緊急対策情報・注意喚起 一覧」のウェブページを参照し、注意喚起が行われた場合は、自分のパソコンに該当するソフトウェアが入っているかを確認し、対応してください。
  - （ご参考） 「緊急対策情報・注意喚起 一覧」（IPA）
    http://www.ipa.go.jp/security/announce/alert.html
  - 「脆弱性が発見されてから、その修正プログラムが公開されるまでの期間」は、脆弱性を解消できない状態となります。この期間を狙う攻撃を「ゼロデイ攻撃」と呼び、防御することが非常に難しく、流行した場合はインターネットを利用することが危険な状態となります。
    「ゼロデイ攻撃」に対しては、修正プログラムが提供されるまでは脆弱性を解消できないため、できる限りの「回避策」を取ることで対応します。「回避策」は、問題となっているソフトウェアによって様々です。例えば、該当ソフトウェアの設定を変更して問題のある機能を停止する、該当ソフトウェアを悪用されないようパソコンから削除するといった対処があります。
    上記の「緊急対策情報・注意喚起 一覧」のウェブページでは、「ゼロデイ攻撃」に関する情報も発信しています。「回避策」を取ることで他の機能に影響を及ぼす場合もありますので、情報をよく確認した上で、対応してください。
  - 「ゼロデイ攻撃」についての詳細は、下記のウェブページを参照してください。
    （ご参考）「修正プログラム提供前の脆弱性を悪用したゼロデイ攻撃について」（IPA）
    http://www.ipa.go.jp/security/virus/zda.html